7/5/1 (Item 1 from file: 2)
DIALOG(R)File 2: INSPEC

11262726
Title: Improved impossible differential attacks on large-block Rijndael
Author(s): Lei Zhang; Wenling Wu; Je Hong Park; Bon Wook Koo; Yongjin Yeom
Author Affiliation: Inst. of Software, Chinese Acad. of Sci., Beijing, China
Inclusive Page Numbers: 298-315
Publisher: Springer-Verlag, Berlin
Country of Publication: Germany
Publication Date: 2008
Conference Title: Information Security. 11th International Conference, ISC 2008
Conference Date: 15-18 Sept. 2008
Conference Location: Taipei, Taiwan
ISBN: 978-3-540-85884-3
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: In this paper, we present some improved impossible differential attacks on large-block Rijndael whose block sizes are larger than 128 bits. First of all, we present some important observations which help us to significantly improve the impossible differential attacks on large-block Rijndael proposed by Nakahara-Pavao (ISC 2007). Then we introduce some new impossible differentials for large-block Rijndael. Utilizing these longer impossible differential distinguishers, **together** with the technique of changing the order of MixColumns and **AddRoundKey** operations proposed by Zhang-Wu-Feng (ICISC 2007), we can apply impossible differential attacks up to 7-round Rijndael-160, 8-round Rijndael-192, and 9-round Rijndael-224/256. As far as we know, except the attack on Rijndael-256, all the other results are the best cryptanalytic results on large-block Rijndael. (*25 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: cryptography
Identifiers: impossible differential attacks; large-block Rijndael; cryptanalytic; block cipher
Classification Codes: B6120D (Cryptography); C6130S (Data security)
INSPEC Update Issue: 2008-044

11/5/1 (Item 1 from file: 144)
DIALOG(R)File 144: Pascal

16548622 PASCAL No.: 04-0196594

Parity-based **concurrent** error detection of substitution-permutation network **block ciphers**

CHES 2003 : cryptographic hardware and embedded systems : Cologne, 8-10 September 2003

KARRI Ramesh; KUZNETSOV Grigori; GOESSEL Michael
WALTER Colin D, ed; KOC Cetin K, ed; PAAR Christof, ed
Department of Electrical and Computer Engineering Polytechnic University, 6 Metrotech Center, Brooklyn, NY 11201, United States; Institute of Computer Science, Fault Tolerant Computing Group University of Potsdam D-, 14439 Potsdam, Germany

Cryptographic hardware and embedded systems. International workshop, 5 (Cologne DEU) 2003-09-08
Journal: Lecture notes in computer science, 2003, 2779 113-124

ISBN: 3-540-40833-9 ISSN: 0302-9743 Availability: INIST-16343; 354000117806090090
No. of Refs.: 22 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English

Deliberate injection of faults into cryptographic devices is an effective cryptanalysis technique against symmetric and asymmetric encryption algorithms. In this paper we will describe parity code based **concurrent** error detection (CED) approach against such attacks in substitution-permutation network (SPN) symmetric **block ciphers** (22). The basic idea compares a carefully modified parity of the input plain text with that of the output cipher text resulting in a simple CED circuitry. An analysis of the SPN symmetric **block ciphers** reveals that on one hand, permutation of the round outputs does not alter the parity from its input to its output. On the other hand, exclusive-or with the round key and the non-linear substitution function (**s-box**) modify the parity from their inputs to their outputs.
In order to change the parity of the inputs into the parity of outputs of an SPN encryption, we exclusive-or the parity of the SPN round function output with the parity of the round key. We also add to all **s-boxes** an additional 1-bit binary function that implements the combined parity of the inputs and outputs to the **s-box** for all its (input, output) pairs. These two modifications are used only by the

CED circuitry and do not impact the SPN encryption or decryption. The proposed CED approach is demonstrated on a 16-input, 16-output SPN symmetric **block cipher** from (1).

English Descriptors: Boarded computer; Error detection; Permutation; Cryptography; Cryptanalysis; Safety; Text; Parity; Block ciphering; Hand; Box; Decryption; Asymmetry; Input output; Non linear function; Fault injection; Attack

French Descriptors: Calculateur embarque; Detection erreur; Permutation; Cryptographie; Cryptanalyse; Securite; Texte; Parite; Cryptage bloc; Main ; Boite; Decryptage; Asymetrie; Entree sortie; Fonction non lineaire; Injection faute; Attaque

Classification Codes: 001D02B01; 001D04A04E

11/5/4 (Item 4 from file: 144)
DIALOG(R)File 144: Pascal

16118773 PASCAL No.: 03-0277405

Hardware design and analysis of **block cipher** components
Information security and cryptology - ICISC 2002 : Seoul, 28-29 November 2002, revised papers

LU XIAO; HEYS Howard M
PIL JOONG LEE, ed; CHAE HOON LIM, ed
Electrical and Computer Engineering, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, NF, A1B 3X5, Canada
International conference on information security and cryptology, 5 (Seoul KOR) 2002-11-28
Journal: Lecture notes in computer science, 2003, 2587 164-181

ISBN: 3-540-00716-4 ISSN: 0302-9743 Availability: INIST-16343; 354000108514350120
No. of Refs.: 22 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English
This paper describes the efficient implementation of Maximum Distance Separable (MDS) mappings and Substitution-boxes (**S-boxes**) in gate-level hardware for application to Substitution-Permutation Network (SPN) **block cipher** design. Different implementations of parameterized MDS mappings and **S-boxes** are evaluated using gate count as the space complexity measure and gate levels traversed as the time complexity measure. On this basis, a method to optimize MDS codes for hardware is introduced by considering the complexity analysis of bit **parallel** multipliers. We also provide a general architecture to implement any invertible **S-box** which has low space and time complexities. As an example, two efficient implementations of **Rijndael**, the **Advanced Encryption Standard** (**AES**), are considered to examine the different tradeoffs between speed and time.

English Descriptors: Encryption; **Parallel** algorithm; Time complexity ; Cryptanalysis; Space complexity; Complexity measure; Block ciphering

11/5/7 (Item 7 from file: 144)
DIALOG(R)File 144: Pascal

13652260 PASCAL No.: 98-0359381

Serpent : A new **block cipher** proposal
FSE : fast software encryption : Paris, 23-25 March 1998

BIHAM E; ANDERSON R; KNUDSEN L
VAUDENAY Serge, ed
Technion, Haifa, Israel; Cambridge University, United Kingdom; University of Bergen, Norway
International workshop on fast software encryption, 5 (Paris FRA) 1998-03-23
Journal: Lecture notes in computer science, 1998, 1372 222-238

ISBN: 3-540-64265-X ISSN: 0302-9743 Availability: INIST-16343; 354000078893800150
No. of Refs.: 22 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English
We propose a new **block cipher** as a candidate for the **Advanced Encryption Standard** . Its design is highly conservative, yet still allows a very efficient implementation. It uses the well-understood DES **S-boxes** in a new structure that **simultaneously** allows a more rapid avalanche, a more efficient bitslice implementation, and an easy analysis that enables us to demonstrate its security against all known types of attack. With a 128-bit block size and a 256-bit key, it is almost as fast as DES on a wide range of platforms, yet conjectured to be at least as secure as three-key triple-DES.

English Descriptors: Cryptography; Safety; Implementation; Cryptographic key

French Descriptors: Cryptographie; Securite; Implementation; **Block cipher**; Linear cryptanalysis; Differential cryptanalysis; Cle cryptographique

Classification Codes: 001D04A04E

11/5/8 (Item 1 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000497624 IP Accession No: 2008017229
Advanced encryption standard (AES) hardware cryptographic engine

Snell, Dorian L
, USA
Publisher Url: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u =/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=72 95671.PN.&OS=pn/7295671&RS=PN/7295671

Document Type: Patent
Record Type: Abstract
Language: English
File Segment: ANTE: Abstracts in New Technologies and Engineering

Abstract:
A cryptographic method and related implements the **Rijndael**- **AES** encryption standard. In one improvement, the decryption round keys are generated on a round by round basis from the final Nk round keys saved from a previous encryption key scheduling operation. Latency and memory requirements are thereby minimized. **S-boxes** for the **AES** key generation and cipher operation itself, may be implemented multiple times in different ways with different power signatures, with a pseudo-random selection of the pathway for the different bytes to be substituted. The premix operation occurs **simultaneously** with the generation of first round keys, and a dummy circuit with substantially identical timing as the real premix circuitry adds power consumption noise to the premix.

Descriptors: Keys; Encryption; Cryptography; Standards; Hardware; Power consumption; Circuits; Scheduling; Dummies; Time measurements; Noise; Engines; Pathways; Electric circuits

24/5/4 (Item 3 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

0000605040 IP Accession No: 2008327584
Block cipher system for data security

Ehrsam, William Friedrich; Meyer, Carl H W; Powers, Robert Lowell; Prentice, Paul Norman; Smith, John Lynn; Tuchman, Walter Leonard
, USA
Publisher Url: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u =/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=39 58081.PN.&OS=pn/3958081& RS=PN/3958081

Document Type: Patent
Record Type: Abstract
Language: English
File Segment: ANTE: Abstracts in New Technologies and Engineering

Abstract:
A device for ciphering message blocks of data bits under control of a cipher key. The cipher device performs an enciphering process for each message block of data by carrying out a predetermined number of iteration operations in the first of which a first half of the message block of data bits is first expanded by duplicating predetermined ones of the data bits. The data bits of the expanded message block are combined by modulo-2 **addition** with an equal **number** of cipher key bits, selected in accordance with an arbitrary but fixed permutation, to produce a plurality of multi-bit segments forming the arguments for a plurality of different nonlinear substitution function boxes. The substitution boxes perform a plurality of nonlinear transformation functions to produce a substitution set of bits which are equal in number to the number of data bits in the first half of the message block. The substitution set of bits is then subjected to a linear transformation in accordance with an arbitrary but fixed permutation. The combined nonlinear transformation and linear transformation results in a product **block cipher** of the first half of the message block. The second half of the message block is then modified by modulo-2 addition with the product **block cipher** of the first half of the message block to produce a modified second half of the message. The modified second half of the message block then replaces the first half of the message block which at the **same time** replaces the second half of the message block in preparation for the next iteration operation. During the next iteration operation, the cipher **key** bits are **shifted** according to a predetermined shift schedule to provide a new set of permuted cipher key bits. The modified second half of the message block is then used with the new set of permuted cipher ket bits in a similar product **block cipher** operation, the result of which is used to modify the first half of the message block. The modified first half of the message block then replaces the modified second half of the message block which at the **same time**

replaces the first half of the message block in preparation for the next iteration operation. During each of the remaining iteration operations of the enciphering process except the last, the cipher **key** bits are **shifted** according to the predetermined shift schedule, a modified half of the message block is remodified according to a product **block cipher** of the previously modified half of the message block and the resulting remodified half of a message block is effectively transposed with the previously modified half of the message block. During the last iteration operation, the cipher **key** bits are **shifted** a last time according to the shift schedule and a last remodification of a modified half of the message block is performed according to a product **block cipher** of the previously modified half of the message block but the resulting remodified half of the message block and the previously modified half of the message block are not transposed and now constitute the enciphered version of the original message block. Deciphering an enciphered message block is carried out by the same series of iteration operations under control of the same cipher **key shifted** during the iteration operations according to a predetermined shift schedule in a direction opposite to that in the enciphering process to reverse the enciphering process and undo every iteration that was carried out in the enciphering process to produce a resulting message block identical with the original message block.

Descriptors: Blocking; Messages; Schedules; Nonlinearity; Transformations; Permutations; Linear transformations; Reproduction; Security; Business machines; Forming

16/3,K/3 (Item 3 from file: 484)
DIALOG(R)File 484: Periodical Abs Plustext

06370495 **Supplier Number:** 566569191 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard

Landau, Susan
American Mathematical Monthly (IAMM) , v111 n2 , p 89-117 **, p.** 29
Feb 2004
ISSN: 0002-9890 **Journal Code:** IAMM
Document Type: Feature
Language: English **Record Type:** Fulltext; Abstract
Word Count: 11527
TEXT:
...College took a different tack to the same general approach (31). In (29), they pulled **Rijndael** apart, but unlike the king's horses and the king's men, Murphy and Robshaw were able to put the algorithm back **together** again. The revision showed a possible direction for attack.

Since the same constant is **added** to each **byte** in the S-box, while the rest of the round function consists of **row shifts**, multiplication by a matrix in GF(2 sup 8), and key **addition**, Murphy and Robshaw suggested that **Rijndael**'s round operations could be regrouped by putting the addition, appropriately modified, into the key...